ABSTRACT OF THE DISCLOSURE

[0018] The invention describes a method for hardening a security mechanism against physical intrusion attacks and against substitution attacks. A user establishes a connection between a network peripheral device (12) and a network (14) via a security mechanism (10) that provides the security functions necessary to access the resources of the network (14). The security mechanism (10) includes a read only memory (ROM) (22) that contains the bootstrap application code that initiates the operation of the mechanism as well as performs the required authentication functions. A persistent memory (24) contains configuration information that enables the security mechanism to configure the device to the network. A volatile memory (26) stores user and device identification information that remains valid only for a given session and is erased thereafter so that a past successful connection won't facilitate a future security breach. A tamper-evident enclosure (32) surrounds the memory elements to provide physical security, which if breached, becomes readily apparent to the user. The software stored in the ROM (22) must be constructed so that a future compromise of the device will not adversely affect the security of past sessions and so that any data that will affect the level of security provided to the user is obtained from the user at the beginning of each session.